CLAIMS

1. An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that an intermediate result be generated; and

execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, and configured to generate said intermediate result.

2. The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

an encryption operation, said encryption operation comprising encryption of one or more plaintext blocks to generate a corresponding one or more ciphertext blocks.

3. The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

a decryption operation, said decryption operation comprising decryption of one or more ciphertext blocks to generate a corresponding one or more plaintext blocks.

4. The apparatus as recited in claim 1, wherein said execution logic is configured to interpret an intermediate result field within a control word which is referenced by said cryptographic instruction.

5. The apparatus as recited in claim 4, wherein said intermediate result field directs said execution logic to generate said intermediate result.

6. The apparatus as recited in claim 4, wherein said intermediate result field directs said execution logic to generate a normal result.

7. The apparatus as recited in claim 1, wherein said execution logic is configured to interpret a round count field within a control word which is referenced by said cryptographic instruction.

8. The apparatus as recited in claim 7, wherein the value of said round count field prescribes a number of cipher rounds to be performed on an input block during execution of said one of the cryptographic operations.

9. The apparatus as recited in claim 1, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

10. The apparatus as recited in claim 1, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

11. The apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references one or more registers within said computing device.

12. The apparatus as recited in claim 11, wherein said one or more registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of one or more input text blocks upon which said one of the cryptographic operations is to be accomplished.

13. The apparatus as recited in claim 11, wherein said one or more registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding one or more output text blocks, said corresponding one or more output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon one or more input text blocks.

14. The apparatus as recited in claim 11, wherein said one or more registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within one or more input text blocks.

15. The apparatus as recited in claim 11, wherein said one or more registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

16. The apparatus as recited in claim 11, wherein said one or more registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising a initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations.

17. The apparatus as recited in claim 11, wherein said one or more registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises:

an intermediate result field, configured to specify whether a normal result or said intermediate result is to be generated during execution of said one of the cryptographic operations.

18. The apparatus as recited in claim 1, wherein said execution logic comprises:

a cryptography unit, configured execute a plurality of cryptographic rounds on each of one or more input text blocks to generate a corresponding each of one or more output text blocks, wherein said plurality of cryptographic rounds are prescribed by a round count field within a control word that is provided to said cryptography unit.

19. An apparatus for performing cryptographic operations, comprising:

a control word, configured to prescribe that an intermediate result be generated during execution of one of the cryptographic operations; and

a cryptography unit within a device, configured to execute said one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also references said control word.

20. The apparatus as recited in claim 19, wherein said control word is stored in memory, and wherein a memory location of said control word is prescribed by contents of a register that is referenced by said cryptographic instruction.

21. The apparatus as recited in claim 19, wherein said cryptography unit executes said one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

22. The apparatus as recited in claim 19, wherein said cryptography unit interprets an intermediate result field within said control word to determine whether to generate a normal result or said intermediate result.

23. The apparatus as recited in claim 19, wherein said cryptography unit interprets a round count field within said control word to determine how many block cipher rounds to execute on a block of input text during execution of said one of the cryptographic operations.

24. The apparatus as recited in claim 19, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

25. A method for performing cryptographic operations in a device, the method comprising:

via a cryptographic instruction, prescribing that an intermediate result be generated during execution of one of a plurality of cryptographic operations; and

receiving the cryptographic instruction, and generating the intermediate result when executing the one of the cryptographic operations.

26. The method as recited in claim 25, wherein said prescribing comprises:

via a first field within a control word that is referenced by the cryptographic instruction, specifying whether a normal result or the intermediate result is to be generated.

27. The method as recited in claim 25, wherein said receiving comprises:

loading the control word from memory.

28. The method as recited in claim 25, said receiving comprises:

executing the one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

29. The apparatus as recited in claim 22, wherein said prescribing comprises:

providing the cryptographic instruction according to the x86 instruction format.

30. The method as recited in claim 25, wherein said prescribing comprises:

via a second field within a control word that is referenced by the cryptographic instruction, specifying how many cipher rounds are to be executed during execution of the one of the cryptographic operations on a block of input text.